(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 528 572 A1**

(12) **EUROPEAN PATENT APPLICATION**

(21) Application number : **92307041.1**

(51) Int. Cl.[5] : **H04L 29/06**

(22) Date of filing : **03.08.92**

(30) Priority : **16.08.91 ZA 916493**
07.05.92 ZA 923306

(43) Date of publication of application :
24.02.93 Bulletin 93/08

(84) Designated Contracting States :
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant : **CONTROL LOGIC (PROPRIETARY) LIMITED**
270 Brickfield Road
Durban Natal Province (ZA)

(72) Inventor : **Pucci, Franco Giovanni**
32 Mountainrise Road, Carrington Heights
Durban, Natal Province R S A (ZA)
Inventor : **Moore, David Thomas**
2 Mahler Close, Hatchwarren
Basingstoke, Hampshire (GB)
Inventor : **Celine, David Harry**
16 Brookland Crescent, Durba North
Natal Province R S A (ZA)
Inventor : **Gani, Abdul Rehman**
5 Belvedere Place
Westville, Natal Province R S A (ZA)

(74) Representative : **Barlow, Roy James**
J.A. KEMP & CO. 14, South Square, Gray's Inn
London WC1R 5LX (GB)

(54) Device for encoding or decoding of signals.

(57) An electronic device comprises coding logic to code digital signals in accordance with one of a number of predetermined codes ; a code selector to select one of the predetermined codes ; and a protocol selector to configure coded digital output signals produced by the coding logic to conform to one of a number of predetermined protocols.

EP 0 528 572 A1

THIS INVENTION relates to an electronic device for encoding or decoding electrical signals.

BACKGROUND TO THE INVENTION

In certain applications such as remote alarm systems and access control systems, which require secure data transmission, data in encrypted form is transmitted by a transmitter to a receiver. The received encrypted data is then decrypted, validated by a control unit, and then further processed according to the requirements of the application.

Various methods of data encryption are known in the art. In most methods, data is encrypted at the transmitter by combining it together with an encryption key according to a fixed algorithm. The encrypted data is decrypted at the receiver by applying a converse algorithm to the encrypted data together with the same encryption key. The security of such a communication system will obviously be compromised if the encryption key becomes known to unauthorised users.

The security of encrypted data transmission may be increased in various ways. For example, the encryption key may be made to vary randomly and used only once. Such an encryption key is known as a "one time key". Alternatively, the encryption key may be fixed and the data to be combined with the key may be varied. This method of data encryption is known in the art as "code hopping".

Both of these methods of data encryption will ensure that no two data transmissions are identical. This principle ensures that encrypted data which is intercepted during transmission and which is subsequently retransmitted by an unauthorised user, cannot be used to disable the alarm system or to bypass the access control system.

Japanese Patent Number 63-155930 discloses a method of providing encrypted data for secure transmission across a public data network. The method comprises generating an encryption key, and the transmission of the key from the transmitter to the receiver, or vice-versa, across the public data network. Network processors at the transmitter and receiver then encrypt and decrypt data transmitted across the network by using the common encryption key. The network processors also format the encrypted data according to a fixed protocol suitable for transmission across the network.

Further methods and apparatus for secure communication are disclosed in the following patent numbers: WO 89/10666 which relates to a protocol which is used for the transmission of encrypted data; GB 2124856 which relates to a multi-level encryption scheme applicable to the broadcasting of encrypted signals; and EP 0300824 which discloses a method of producing a continuous sequence of one-time encryption keys.

Japanese Patent number 61-205048 relates to a communication apparatus which is configurable to receive or transmit data according to one of a number of different selectable communication protocols. The data is not encrypted prior to transmission by the communication apparatus.

The efficiency of data encryption using code hopping techniques is reduced when data encryption is performed using standard types of integrated circuits, because the word length of these integrated circuits is small. This is problematic in instances where more alarm systems or access control systems are manufactured than there are distinct codes available, as duplication is inevitable and security is thereby reduced.

In one particular type of remote alarm system, the number of distinct codes is increased by widening the word length of the algorithms used for encryption and decryption. When this is done by using discrete standard types of integrated circuits, the resulting electronic circuits for encryption and decryption are large, complex, unnecessarily expensive and have large power consumptions.

OBJECT OF THE INVENTION

It is an object of this invention to provide a device which will enable the encryption or decryption of electrical signals.

SUMMARY OF THE INVENTION

According to this invention there is provided an electronic coding device, comprising :

coding logic means to code digital signals in accordance with one of a number of predetermined codes;

a code selector connected to the coding logic means, the code selector being instructable to select one of the number of predetermined codes;

an input for the coding logic means to receive digital input signals; and

a protocol selector connected to the coding logic means, the protocol selector being instructable to configure coded digital output signals produced by the coding logic means to conform to one of a number of predetermined protocols.

Preferably, the code and protocol selectors are a configuration store, and the configuration store contains a number of key values, a number of variable values, and data to select one of the number of predetermined codes for coding digital signals.

A yet further feature of the invention provides for one coding of digital signals is encrypting a key value and a variable value contained in the configuration store, to produce an encrypted signal, and another coding of digital signals is decrypting a previously encrypted signal to recover from it the variable value by

using the same key value contained in the configuration store, which was used for encryption.

Still further features of the invention provide for the configuration store to be connectable to an instructing means for generating instruction inputs to the store, for selectable values and data in the configuration store to be accessible and alterable by the instruction means, and for the configuration store to be a memory. The memory may be a non-volatile, electrically-erasable, programmable, read-only memory.

Also, the encoded digital output signal is configurable to be a binary signal which alternates between an "off" state and an "on" state, each time a signal is decrypted.

There is also provided for the digital output signal to be configurable to be a pulse signal of selectable duration, each time a signal is decrypted.

Further there is provided for a means for indicating a low supply. voltage to the device, a means for indicating a malfunction of the electrically-erasable, programmable, read-only memory, and a means for indicating any of the key values contained in the configuration store, in encrypted form.

The invention extends to provide a method of configuring an electronic coding device comprising:
interfacing on instructing means to a code selector and to a protocol selector, said selectors being connected to a coding logic means for coding digital signals in accordance with one of a number of predetermined codes;
instructing the code selector to select one of the number of predetermined codes; and
further instructing the protocol selector to selectively configure coded digital output signals produced by the coding logic means to conform to one of a number of predetermined protocols.

There is also provided for instructing the code selector to select one of the number of predetermined codes by storing a number of key values, and a number of variable values in a configuration store in the coding logic means.

There is also provided for coding digital signals by encrypting a key value and a variable value contained in the configuration store, to produce an encrypted signal, or by decrypting a previously encrypted signal to recover from it the variable value by using the same key value contained in the configuration store, which was used for encryption.

There is also provided for selectively configuring the coding logic means to be connectable to one of a number of predetermined signal transmission means.

There is also provided for linking one coding device configured for decryption, to a number of coding devices configured for encryption, to form an operable set of coding devices, by storing a different key value into the configuration store of each of the encryption coding devices, and by storing all of these different key values into the configuration store of the decryption coding device.

There is also provided for synchronising an operable set of coding devices by initialising the variable value stored in the configuration store of each of the coding devices, to be a known, preselected value.

The is also provided for avoiding the need for resynchronising an operable set of coding devices, when power is removed from any coding device in the set, by storing the configuration of each coding device in a non-volatile memory in that coding device.

BRIEF DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the invention is described below, by way of example only, and with reference to the accompanying drawings, in which:

Figure 1 is a perspective view of a packaged integrated circuit;

Figure 2 is a schematic representation of the pin layout of the integrated circuit of Figure 1;

Figure 3 is a schematic block diagram of the integrated circuit of Figure 1;

Figure 4 is a block diagram of coding logic for encrypting digital signals;

Figure 5 is a block diagram of coding logic for decrypting digital signals; and

Figure 6 is a block diagram of a programmer for configuring the integrated circuit of Figure 1.

DETAILED DESCRIPTION Of THE DRAWINGS

Referring to Figure 1, an electronic coding device is represented generally by numeral (21) and is, in this embodiment, an integrated circuit. The integrated circuit comprises a small wafer of semiconductor material (not shown), such as silicon, on which an electrical circuit is produced by means any one of a number of lithographic techniques which are well known in the art. The semiconductor wafer is encapsulated in a rectangular block of insulating plastics or ceramic material (22) to provide a degree of structural and environmental protection. Electrical connection to the semiconductor wafer is provided by a number of metallic pins (23), each pin protruding from the encapsulating block (22) and being in electrical contact with the semiconductor wafer. The pins (23) are arranged in two rows on opposing sides of the encapsulating block (22). The configuration of the pins indicated in Figure 1 is utilised for surface-mounting the integrated circuit (21) to a printed circuit board (not shown).

The pin configuration of the integrated circuit is indicated in Figure 2. The pins are arranged in a 20-pin dual-in-line (DIL) configuration and are individually indicated by numerals 1 to 20 in Figure 2. As indicated, only twelve of the pins are used, with the pins numbered 2, 3, 8, 9, 10, 11, 19 and 20 being unused.

Referring now to Figure 3, a block diagram of the

electrical circuit on the semiconductor wafer (not shown) of the integrated circuit of Figure 1, is indicated. The core of the electrical circuit is a microprocessor (24) such as the TMS370 8-bit microprocessor core available from Texas Instruments of Dallas, Texas in the USA. The microprocessor memory comprises 4 kilobytes of read-only memory (ROM) (25), 256 bytes of random-access memory (RAM) (26) and 256 bytes of electrically-erasable programmable read-only memory (EEPROM) (27). The ROM and EEPROM memories are non-volatile so that data stored in these memories is not lost when power is removed from the integrated circuit (21). A crystal oscillator and divide-by-2 clock generator (28) provides clock frequency for the micro-processor (24) while system control is provided by firmware (29). An input/output port (30) provides five general bidirectional input/output lines (31). The input/output lines are individually configurable under program control.

A fuse (32) may be selectively blown to disable external read access to the ROM, RAM and EEPROM memories to protect any sensitive data which might be stored in these memories. The fuse (32) is usually blown only after the integrated circuit (21) has been tested for correct operation after it has been manufactured. For use in applications where power consumption is critical, the integrated circuit (21) has a stopped mode in which all of the circuit activity is stopped but data in the RAM memory (26) is maintained. Data in the non-volatile ROM (25) and EEPROM (27) memories will not be lost in any event. The integrated circuit (21) can only be released from the stopped mode by an externally supplied reset signal.

In one particular application of this integrated circuit, related to its use in remote alarm systems, standard application software is masked into the ROM memory (25) by lithographic techniques at the time of manufacture of the integrated circuit. Referring to Figures 4 and 5, the application software consists of an encryption algorithm (33) and a decryption algorithm (40).

The integrated circuit (21) may be configured to perform either encryption or decryption by enabling either the encryption algorithm (33) or the decryption algorithm (40) respectively.

Configuration data representing the configuration of the integrated circuit is stored in the EEPROM memory (27). The configuration data relates to the mode of operation of the integrated circuit, that is whether the encryption algorithm (33) or the decryption algorithm (40) has been enabled. Further configuration data comprises a fixed, 56-bit key value, or encryption key (34) and a variable value, or counter value (35). An arbitrary fixed data byte (37) is also stored in the EEPROM memory (27).

The operation of the application software in an integrated circuit (21) which has been configured for encryption is described below. When the encryption algorithm (33) is activated, the counter value (35) is incremented and the fixed byte (37) is appended to it. A checksum byte is computed from the counter value (35) and the fixed data byte (37) and is further appended to the counter value. The counter value (35) is 40-bits wide so that when the counter value is appended by the fixed byte (37) and the checksum byte (38), a 56-bit variable is obtained. Any algorithm may be used to compute the checksum, for example, a 16-bit cyclic redundancy check. The counter value, appended by the fixed and the checksum byte is encrypted together with the encryption key (34) by means of the encryption algorithm (33) to produce a unique 56-bit output value at (36). The output value from the encryption algorithm (33) is converted to serial form by a parallel-to-serial converter (39).

The serial data stream produced at the output of the parallel-to-serial converter (39) is transmitted by means of a radio-frequency or an infra-red transmitter front-end (not shown). This output data stream is configurable to conform to the timing waveform requirements of the particular transmitter type which may be used in a given application.

In use, up to four integrated circuits (21) configured for encryption may be linked to a single integrated circuit (21) configured for decryption, to form an operable set of devices. The configuration data of the decryption integrated circuit must provide for the decryption algorithm (40) to be enabled. Furthermore, each of the encryption integrated circuits must be configured with a unique encryption key (34) and with the same fixed data byte (37). The decryption integrated circuit is configured with the encryption key (34) of each of the linked encryption integrated circuits, up to a maximum of four such keys, and with the common fixed data byte (37). The decryption integrated circuit is further configured with a counter value for each of the linked encryption integrated circuits, up to a maximum of four.

A radio-frequency of infra-red receiver (not shown) acts as a front-end to the integrated circuit (21) which is configured for decryption, to receive a data stream transmitted by any one of the encryption integrated circuits. The receiver type is selected to match the transmitters used with the encryption integrated circuits.

The operation of the application software in an integrated circuit which has been configured for decryption is described in the discussion which follows. A serial data stream which is received by the receiver front-end (not shown) is converted into a received 56-bit data word by a serial-to-parallel converter (41). The data word is decrypted by applying the decryption algorithm (40) and a decryption key (42a). It will be obvious to a person skilled in the art that where the decryption algorithm (40) is the inverse of the encryption algorithm (33), and where the decryption key (42a) is the same as the encryption key (34), then

the decrypted data word will be a 56-bit data word made up of the counter value (35), followed by the fixed byte (37) and the checksum byte (38) which was transmitted in encrypted form as described above.

An additional checksum byte is computed from the decrypted counter value and the decrypted fixed byte using an identical algorithm to the checksum algorithm that was used prior to encryption to compute the checksum byte (38). The received checksum byte and the computed checksum byte are compared at (43) and, if they are not the same, then either data corruption has occurred during transmission, or an incorrect decryption key has been used in the decryption process. If the received and computed checksum bytes do not match, the received data word is again decrypted using another decryption key (42b) stored in the EEPROM memory (27) of the decryption integrated circuit and a checksum byte is computed and compared with the received checksum byte as above. The process is repeated until either all the stored decryption keys (42a), (42b), (42c) and (42d) have been used for decryption, or a computed checksum byte is found which matches the received, decrypted checksum byte. If no matching checksum bytes are found in this manner, the received data is discarded and the receiver continues to listen for other transmitted streams of data.

When matching checksum bytes are found, the received, decrypted fixed byte is compared at (44) against the fixed byte stored in the EEPROM (27) of the decryption integrated circuit. If the received and the stored fixed bytes do not match, the received data is discarded.

Lastly, the received, decrypted counter value is tested at (45) for validity against the stored counter value corresponding to the encryption key (42a), (42b), (42c) or (42d) which produced matching checksum bytes. For the received, decrypted counter value to be valid, it must be greater than the corresponding counter value stored in the decryption integrated circuit, since the counter value (35) in the encryption integrated circuit is incremented, prior to encryption and transmission. In addition the received counter value must be less than the stored counter value plus a deadband of 2047, to allow for accidental or deliberate activation of the encryption integrated circuit when it is out of transmission range of the decryption integrated circuit. Once the received counter value has been tested and found to be valid, an output signal is generated by the integrated circuit, at (46), according to the requirements of the application.

The output (46) of the decryption integrated circuit (21) may be configured to toggle between two states, equivalent to an "on" or an "off" state, or to be a pulse of selectable duration between 0,1 and 2,5 seconds. Alternatively, the output (46) may be configured to emulate the protocol of other known types of integrated circuits. An output signal (46) conforming to the emulated protocol is generated each time the decryption integrated circuit (21) receives a valid data stream from an encryption integrated circuit. Some of the protocols which may be emulated are the MC145026/VD5026 data format from Motorola of the USA, the MM53200/MM57C200 data format from National Semiconductor of the USA, or the TEA5500/1 data format from Philips of the Netherlands.

Turning now to Figure 6, the EEPROM memory (27) in which the configuration of the integrated circuit (21) is stored, is configured by means of a programming unit (50) which may, optionally, be connected to a computer (57) such as an IBM-compatible personal computer (PC). The programming unit (50) comprises a microprocessor (52), a power supply (53), a keypad (54) for data entry, a liquid crystal display (LCD) (55) and a programming socket (56) to receive the integrated circuit (21). The programming unit (50) may be connected, at (57), to a parallel expansion socket (not shown) for external programming of additional integrated circuits (21). The programming unit (50) is connectable to the computer (51) through an RS232C communication port (58). The programming unit may be used in a stand-alone mode, in which case connection to the PC (51) is not necessary, and all configuration is performed via the keypad (54).

Each integrated circuit (21) which is configured for encryption is configured with its own fixed unique encryption key (34) by generating a 56-bit random number in the programmer (50) and downloading this value to the EEPROM memory (27) of the integrated circuit. A single integrated circuit (21) configured for decryption is linked with up to four integrated circuits configured for encryption, by configuring its EEPROM memory (27) with the respective encryption keys (42a), (42b), (42c) and (42d) of the encryption integrated circuits to which it is to be linked.

The output of an integrated circuit (21) configured for encryption may be used to cause a light-emitting-diode (LED) (not shown) to flash intermittently to provide an indication of low supply voltage. When a low supply voltage is detected, a warning code is transmitted by the encryption integrated circuit to the integrated circuit (21) configured for decryption, to which it is linked, and an output of the decryption integrated circuit will then be set, and this output may be used to illuminate an LED or to sound a buzzer to provide audible and visual warning of the low supply voltage. A similar warning code may be transmitted when an encryption integrated circuit is unable to write data to the EEPROM memory (27) due to a malfunction.

When integrated circuits (21) are used in a motor vehicle alarm system, for example, one or more encryption integrated circuits must be linked with a single integrated circuit configured for decryption in the manner outlined above, that is, the encryption key of each encryption integrated circuit is loaded into the

configuration memory of the decryption integrated circuit where it is then available for use by the decryption algorithm (40). To ensure security, the encryption integrated circuit can be made to flash an LED (not shown) to enable the optical recovery of the encryption key in an integrated form. The encrypted flashes of light may be detected by a receiver and decrypted and down-loaded to a decryption integrated circuit (21). In this manner, a service station may quickly and easily reconfigure the alarm system on a motor vehicle. To ensure synchronisation between the encryption and decryption integrated circuits, in an operable set, all counter values stored in the respective memories of these devices are initialised to have zero values.

This embodiment of the invention has been described with particular reference to a remote alarm system, but the scope of the invention is clearly not limited to this application.

The invention therefore provides a low-cost, configurable application oriented controller suitable for use in applications requiring secure data transmission.

Claims

1. An electronic coding device, comprising:
coding logic means to code digital signals in accordance with one of a number of predetermined codes;
a code selector connected to the coding logic means, the code selector being instructable to select one of the number of predetermined codes;
an input for the coding logic means to receive digital input signals; and
a protocol selector connected to the coding logic means, the protocol selector being instructable to configure coded digital output signals produced by the coding logic means to conform to one of a number of predetermined protocols.

2. An electronic coding device as claimed in claim 1 characterised in that the code selector and the protocol selector are a configuration store.

3. An electronic coding device as claimed in claim 2 characterised in that the configuration store contains a number of key values, a number of variable values, and data to select one of the number of predetermined codes for coding digital signals.

4. An electronic coding device as claimed in claim 3 characterised in that one coding of digital signals is encrypting a key value and a variable value contained in the configuration store, to produce an encrypted signal.

5. An electronic coding device as claimed in claim 4 in which another coding of digital signals is decrypting a previously encrypted signal to recover from it the variable value by using the same key value contained in the configuration store, which was used for encryption.

6. An electronic coding device as claimed in any one of claims 2 to 5 characterised in that the configuration store is connectable to an instructing means for generating instruction inputs to the store.

7. An electronic coding device as claimed in claim 6 characterised in that selectable values and data in the configuration store are accessible and alterable by the instruction means.

8. An electronic coding device as claimed in any one of claims 2 to 7 characterised in that the configuration store is a memory.

9. An electronic coding device as claimed in claim 8 characterised in that the memory is a non-volatile, electrically-erasable, programmable, read-only memory.

10. An electronic coding device as claimed in claim 5 characterised in that the digital output signal is configurable to be a binary signal which alternates between an "off" state and an "on" state, each time a signal is decrypted.

11. An electronic coding device as claimed in claim 5 characterised in that the digital output signal is configurable to be a pulse signal of selectable duration, each time a signal is decrypted.

12. An electronic coding device as claimed in any one of the preceding claims characterised in that it includes a means for indicating a low supply voltage to the device.

13. An electronic coding device as claimed in claim 9 characterised in that it includes a means for indicating a malfunction of the electrically-erasable, programmable, read-only memory.

14. An electronic coding device as claimed in any one of claims 3 to 13 characterised in that it includes a means for indicating any of the key values contained in the configuration store, in encrypted form.

15. A method of configuring an electronic coding device comprising:
interfacing on instructing means to a code selector and to a protocol selector, said selectors being

connected to a coding logic means for coding digital signals in accordance with one of a number of predetermined codes;
characterised in that the code selector is instructed to select one of the number of predetermined codes; and
the protocol selector is further instructed to selectively configure coded digital output signals produced by the coding logic means to conform to one of a number of predetermined protocols.

16. A method of configuring an electronic coding device as claimed in claim 15 characterised in that the code selector is instructed to select one of the number of predetermined codes by storing a number of key values, and a number of variable values in a configuration store in the coding logic means.

17. A method of configuring an electronic coding device as claimed in claim 16 characterised in that one of the predetermined codes for coding digital signals is encrypting a key value and a variable value contained in the configuration store, to produce an encrypted signal.

18. A method of configuring an electronic coding device as claimed in claim 17 characterised in that another of the predetermined codes for coding digital signals is decrypting a previously encrypted signal to recover from it the variable value by using the same key value contained in the configuration store, which was used for encryption.

19. A method of configuring an electronic coding device as claimed in any one of claims 15 to 18 characterised in that the coding logic means is selectively connectable to one of a number of predetermined signal transmission means.

20. A method of configuring an electronic coding device as claimed in claim 18 characterised in that one coding device configured for decryption is linked to a number of coding devices configured for encryption, to form an operable set of coding devices, by storing a different key value into the configuration store of each of the encryption coding devices, and by storing all of these different key values into the configuration store of the decryption coding device.

21. A method of configuring an electronic coding device as claimed in claim 20 characterised in that the operable set of coding devices is synchronised by initialising the variable value stored in the configuration store of each of the coding devices, to be a known, preselected value.

22. A method of configuring an electronic coding device as claimed in claim 21 characterised in that the need for resynchronising an operable set of coding devices is avoided, when power is removed from any coding device in the set, by storing the configuration of each coding device in a non-volatile memory in that coding device.

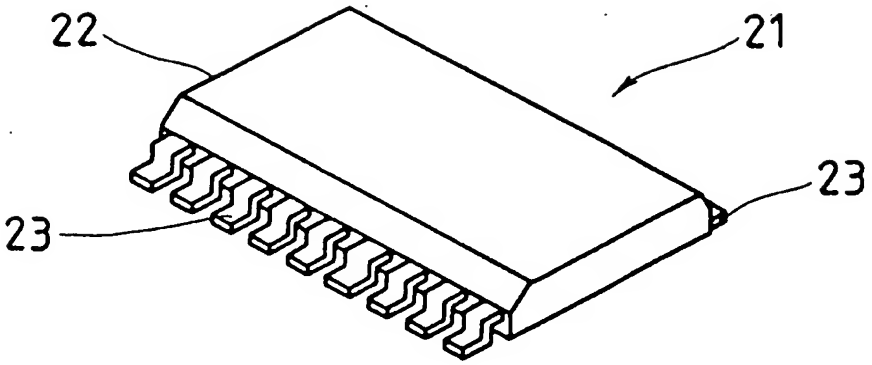
22
21
23
23

FIG. 1

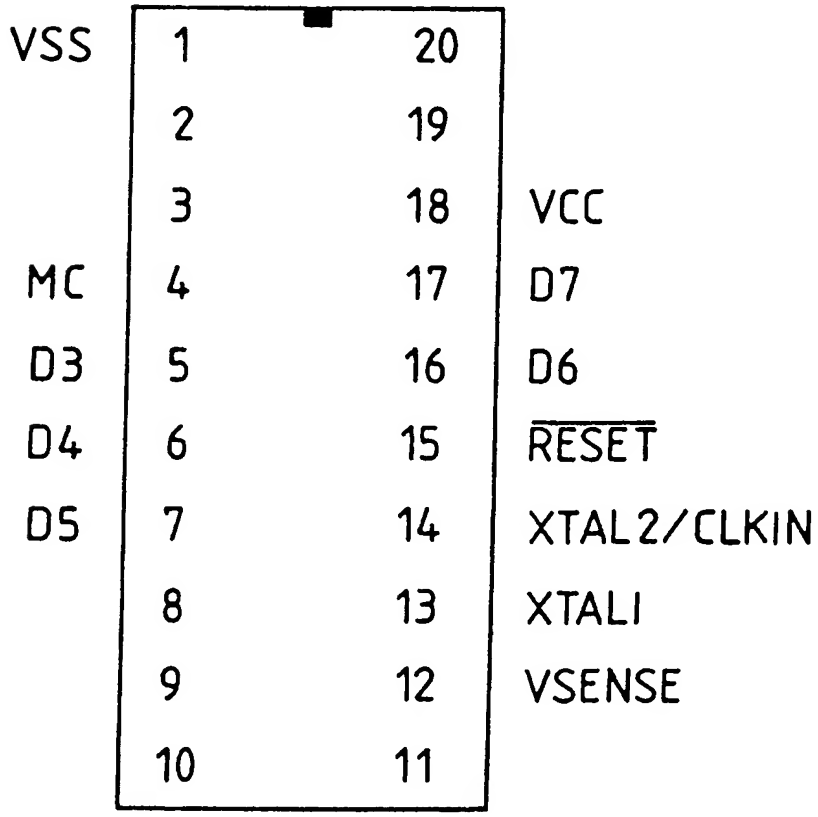
VSS
1
20
2
19
3
18
VCC
MC
4
17
D7
D3
5
16
D6
D4
6
15
RESET
D5
7
14
XTAL2/CLKIN
8
13
XTALI
9
12
VSENSE
10
11

FIG. 2

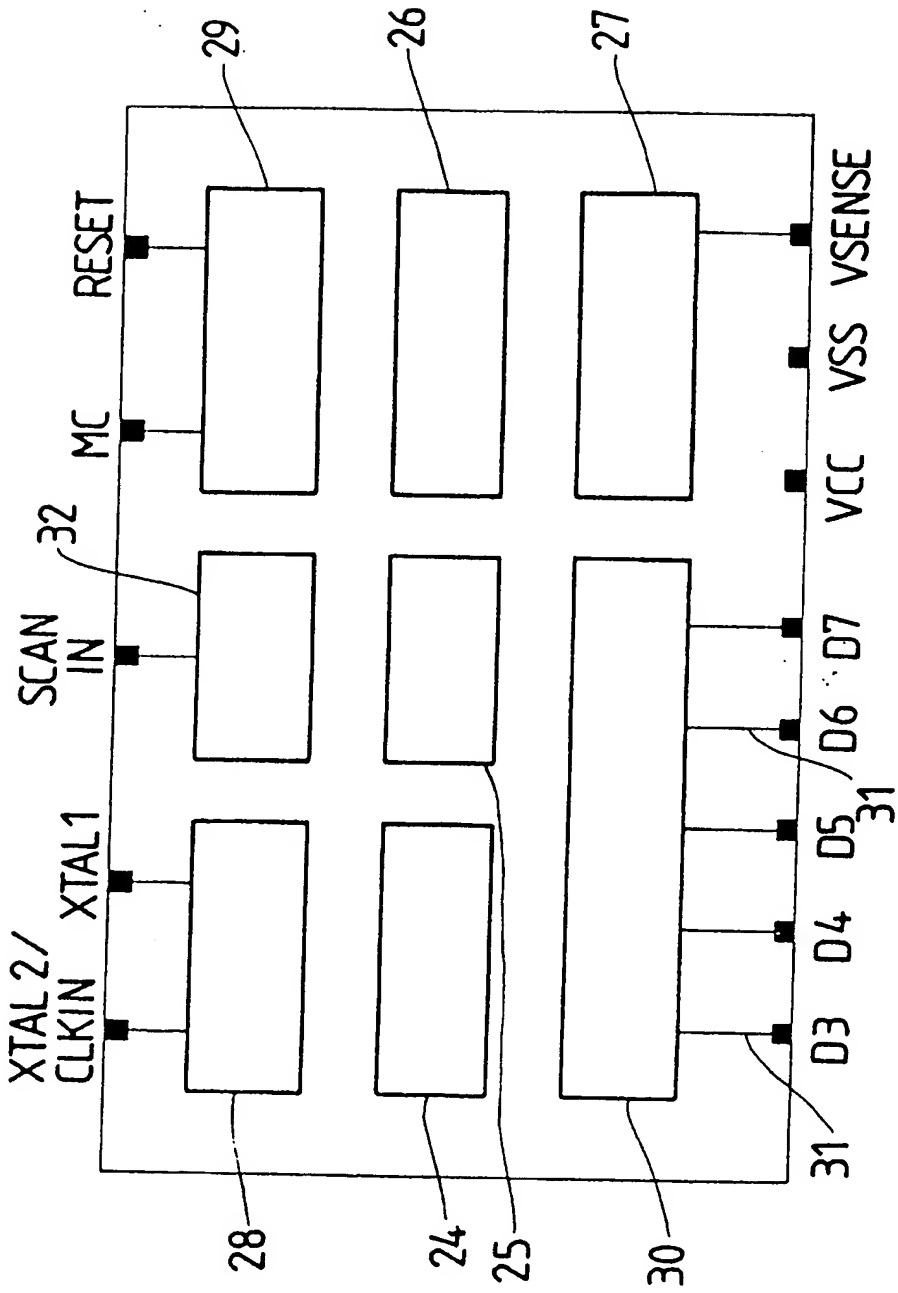
29
26
27
RESET
MC
32
SCAN IN
XTAL1
XTAL2/ CLKIN
VSENSE
VSS
VCC
D7
D6
D5
D4
D3
31
31
28
24
25
30

FIG. 3

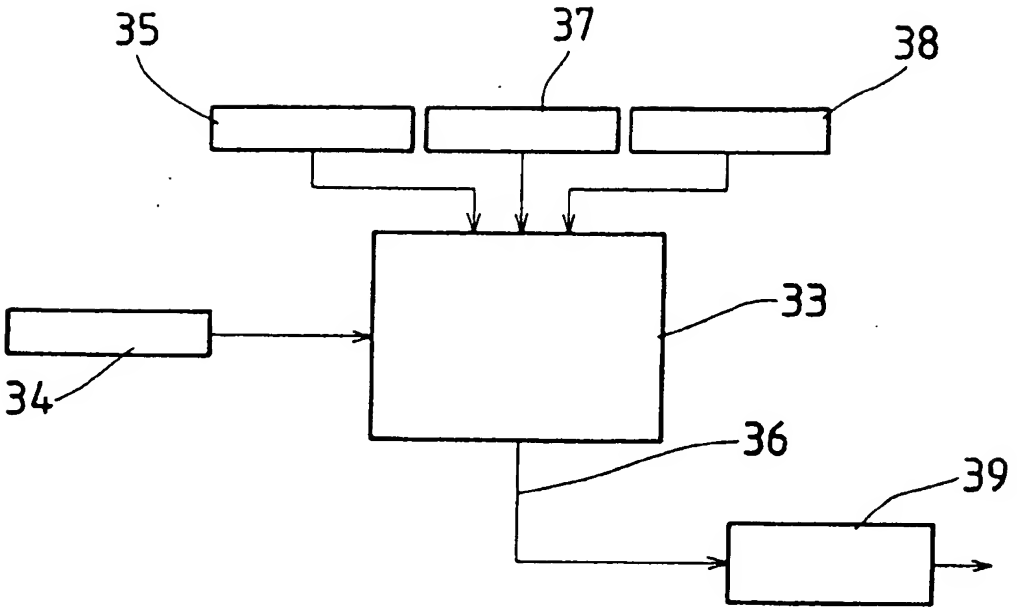

FIG. 4

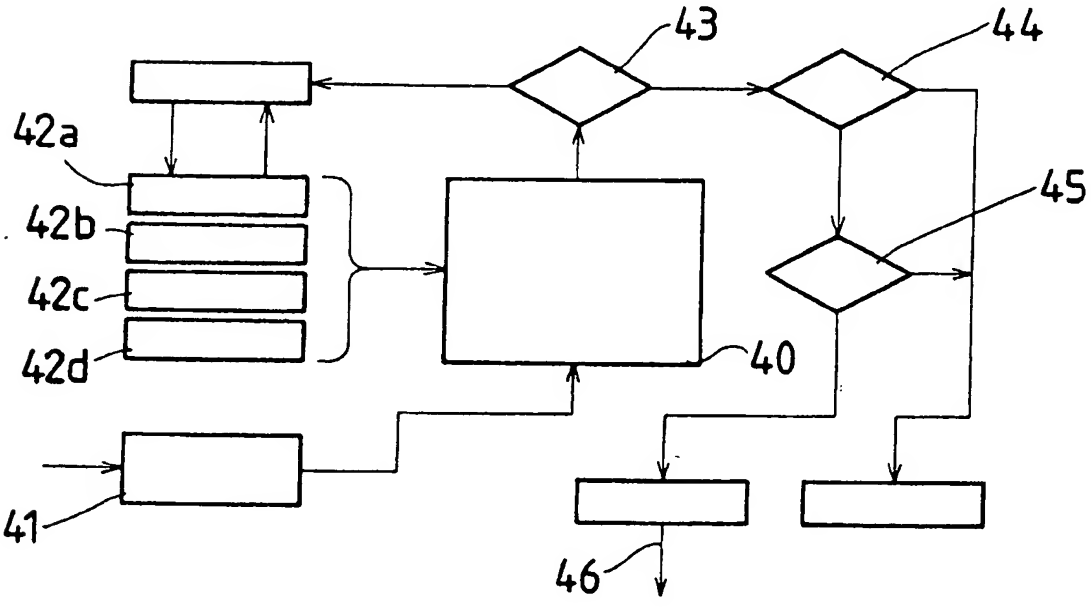

FIG. 5

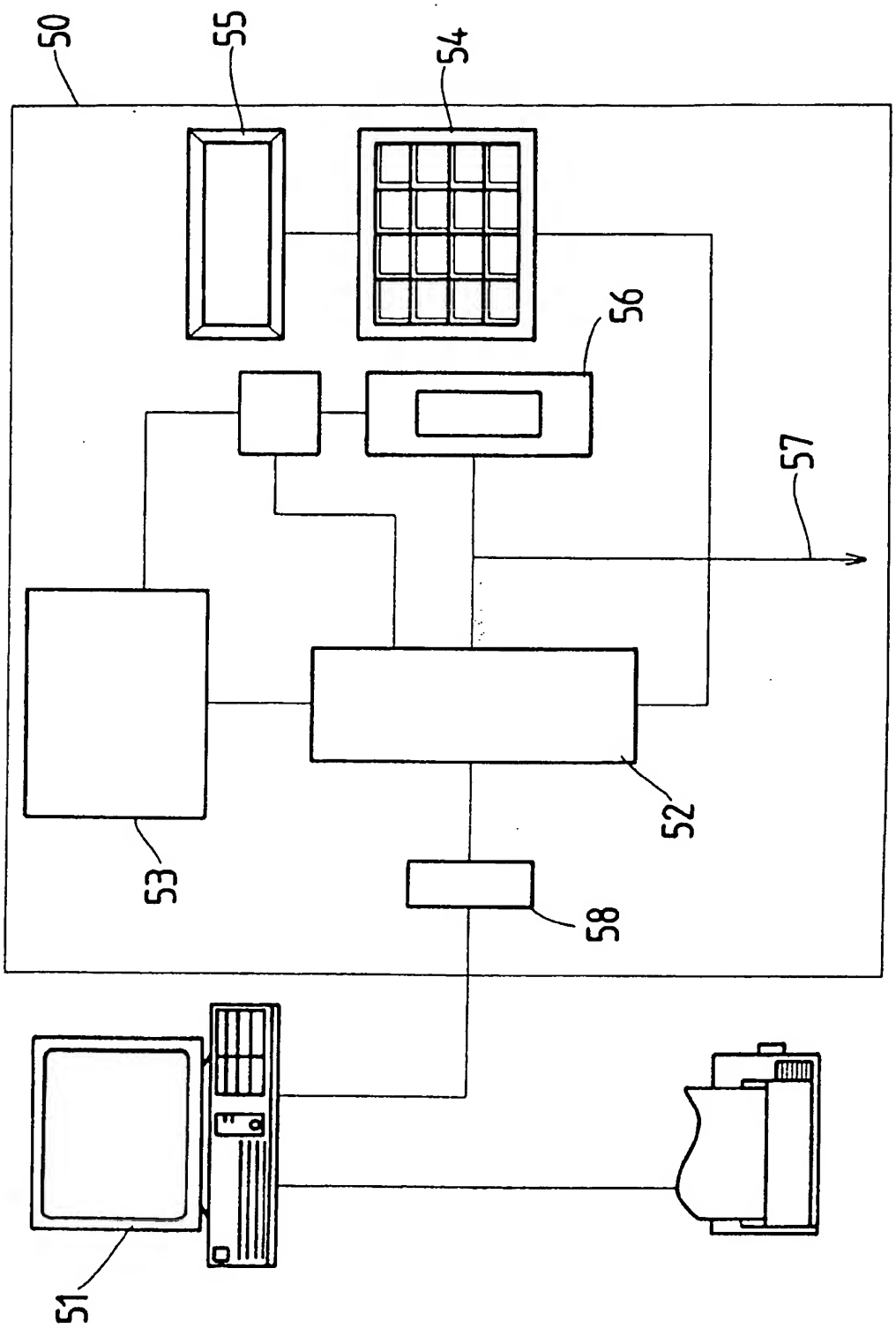

FIG.6

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 92 30 7041

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
X	US-A-4 281 315 (H.C.BAUER ET AL) * column 2, line 17 - line 45 * * claims 1-5 *	1,2,15	H04L29/06
Y		1-5, 15-18	

X	WO-A-8 701 484 (NCR) * page 1, line 29 - page 3, line 9 * * page 5, line 2 - page 8, line 6 * * abstract *	1,2,15	

Y	PHILIPS TELECOMMUNICATION REVIEW vol. 47, no. 3, September 1989, HILVERSUM NL pages 1 - 19 , XP72642 R.C.FERREIRA 'THE SMART CARD: A HIGH SECURITY TOOL IN EDP' * paragraph 4; figure 3 * * paragraph 5 * * paragraph 6 *	1-5, 15-18	
	-----		TECHNICAL FIELDS SEARCHED (Int. Cl.5)
			H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	10 DECEMBER 1992	CANOSA ARESTE C.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0401)